PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-134451
(43)Date of publication of application : 21.05.1999

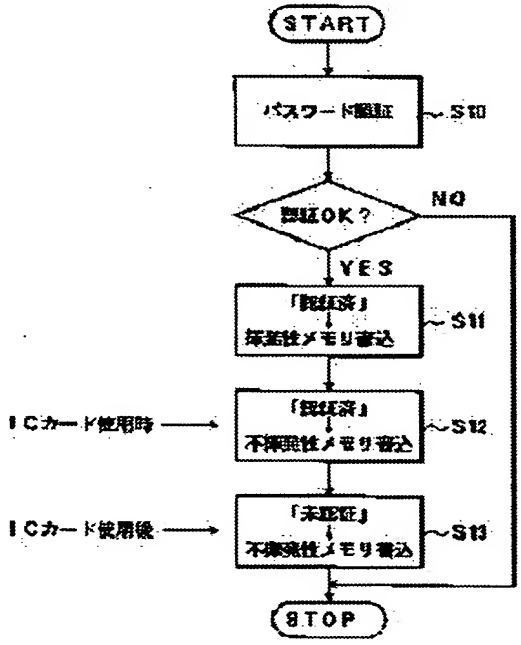
(51)Int.Cl. G06K 17/00
G06K 19/10

(21)Application number : 09-294441
(22)Date of filing : 27.10.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MASUTSUKA KOUJI
YUSA HIROSHI
OMA YASUYUKI
SUZUKI KENICHI

(54) IC CARD, METHOD FOR CHANGING-OVER AUTHENTICATION OF IC CARD, SYSTEM THEREFOR AND RECORDING MEDIUM STORED WITH AUTHENTICATION CHANGE-OVER PROGRAM OF IC CARD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a card from being used evilly by writing a usage possible state in a volatile memory at the time of inputting and authenticating a password, copying the contents of the volatile memory in a non-volatile memory after writing a usage impossible state at the time of pulling-out the card and holding the usage possible state at the time of pulling-out the card.
SOLUTION: The password is requested for the user of an IC card, authentication is executed based on the password which is inputted by the request (S10), 'authenticated' for adopting the IC card as the one in the usage possible state is written in the volatile memory at the time of authentication that a user is justified (S11) and 'authenticated' is also written in the non-volatile memory at the time of using the IC card (S12). Then, the contents of the volatile memory is copied into the non-volatile memory after using the IC card, 'not authenticated' is written in the non-volatile memory and the usage impossible state is held (S13). Thus, the card is prevented from being used evilly.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

4. Japanese Patent Application, Publication No.S62-177696
(No translation provided)

5. Japanese Patent Application, Publication No.H11-134451

[0031] Step 205) The terminal unit 30 performs a settlement process required for purchases or the like of a user, i.e., revises the balance corresponding to a relevant IC card (of a post payment account) by deducting the amount of these purchases or the like from it.
Step 206) When completing the settlement process, the terminal unit 30 executes the "CLEAR STATUS" command so as to have the content in the EEPROM 12 indicate the "yet-to-be-verified" state.
[0032] Step 207) When the user removes the IC card 10 from a card-slot of the terminal unit 30, the content in the RAM 11 changes automatically so as to indicate the "yet-to-be-verified" state as the power supply to the IC card stops. In this manner, it is possible for a user to use an IC card 10 at the terminal unit 30 located in a store without a need of going through a risk of entering his/her password in presence of other people even if the use of the IC card 10 is for a payment in a post payment system, and yet the card automatically turns into the "yet-to-be verified" state once the user completes the use this IC card. As result of this configuration, even if this IC card comes to a possession of other person, he/she cannot use the IC card as he/she does not know what a correct password is.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－134451

(43)公開日　平成11年(1999)５月21日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00		Ｔ
19/10			19/00	Ｒ

審査請求　未請求　請求項の数11　ＯＬ　（全９頁）

(21)出願番号　特願平9－294441

(22)出願日　平成９年(1997)10月27日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　益塚　幸児
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　遊佐　洋
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　大間　康之
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

最終頁に続く

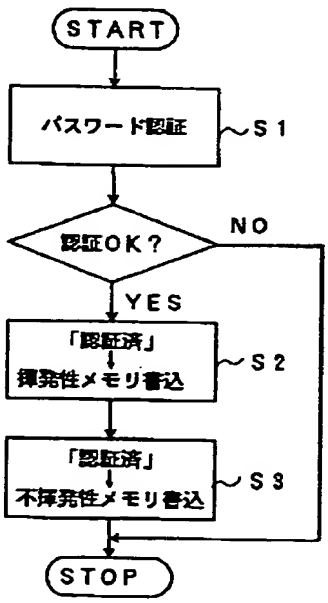
(54)【発明の名称】　ＩＣカード及びＩＣカードの認証切替方法及びシステム及びＩＣカードの認証切替プログラムを格納した記憶媒体

(57)【要約】

【課題】　カードの所有者本人が本人確認を済ませた状態でＩＣかーどを保持しておく状態と、パスワード入力がないと使用不可能状態とする２通りの状態を選択することが可能なＩＣカード及びＩＣカードの認証切替方法及びシステム及びＩＣカードの認証切替プログラムを格納した記憶媒体を提供する。

【解決手段】　本発明は、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い、利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込む共に、前記不揮発性メモリにも「認証済」を書き込む。

本発明の第１の原理を説明するための図



【特許請求の範囲】
【請求項１】　パスワードを入力し、認証することにより使用可能状態となるＩＣカードであって、
パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、
前記揮発性メモリの内容が複写され、カード引抜き時においても使用可能状態を保持する不揮発性メモリとを有することを特徴とするＩＣカード。
【請求項２】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替方法において、
前記ＩＣカードの利用者に対してパスワードを要求し、
入力されたパスワードに基づいて認証を行い、
前記利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込、更に、前記不揮発性メモリにも「認証済」を書き込むことを特徴とするＩＣカード認証切替方法。
【請求項３】　任意のタイミングで、使用可能状態が書き込まれている前記不揮発性メモリの内容を、前記ＩＣカードを使用不可能状態とする「未認証」に書き替える請求項２記載のＩＣカード認証切替方法。
【請求項４】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替方法において、
前記ＩＣカードの利用者に対してパスワードを要求し、
入力されたパスワードに基づいて認証を行い、
前記利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込み、
前記ＩＣカードの使用時に、前記不揮発性メモリにも「認証済」を書き込み、
前記ＩＣカードの使用後、前記不揮発性メモリに「未認証」を書き込むことを特徴とするＩＣカード認証切替方法。
【請求項５】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替システムであって、
前記ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段と、
前記認証手段により前記利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込み、更に前記不揮発性メモリにも「認証済」を書き込む認証情報書込手段とを有することを特徴とするＩＣカード認証切替システム。
【請求項６】　任意のタイミングで、使用可能状態が書き込まれている前記不揮発性メモリの内容を、前記ＩＣカードを使用不可能状態とする「未認証」に書き替える認証情報書替手段を更に有する請求項５記載のＩＣカード認証切替システム。
【請求項７】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替システムであって、
前記ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段と、
前記認証手段により、前記利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込む揮発性メモリ書込手段とを有するバランスリーダと、
前記ＩＣカードの使用時に、前記不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込手段と、
前記ＩＣカードの使用後、前記不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込手段とを有する端末とを有することを特徴とするＩＣカード認証切替システム。
【請求項８】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替プログラムを格納した記憶媒体であって、
前記ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、
前記認証プロセスにより前記利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込み、更に前記不揮発性メモリにも「認証済」を書き込む認証情報書込プロセスとを有することを特徴とするＩＣカード認証切替プログラムを格納した記憶媒体。
【請求項９】　任意のタイミングで、使用可能状態が書き込まれている前記不揮発性メモリの内容を、前記ＩＣカードを使用不可能状態とする「未認証」に書き替える認証情報書替プロセスを更に有する請求項８記載のＩＣカード認証切替プログラムを格納した記憶媒体。
【請求項１０】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使

用不能状態とするＩＣカード認証切替プログラムを格納した記憶媒体であって、
前記ＩＣカードを読み込むバランスリーダに搭載され、
前記ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、
前記認証プロセスにより、前記利用者が正当であると認証された場合に、前記ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込む揮発性メモリ書込プロセスとを有するＩＣカード認証切替プログラムを格納した記憶媒体。
【請求項１１】　パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替プログラムを格納した記憶媒体であって、
前記ＩＣカードの使用時の端末に搭載され、
前記ＩＣカードの使用時に、該ＩＣカードの前記揮発性メモリに「認証済」が書き込まれている場合に、前記不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込プロセスと、
前記ＩＣカードの使用後、前記不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込プロセスとを有することを特徴とするＩＣカード認証切替プログラムを格納した記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード及びＩＣカードの認証切替方法及びシステム及びＩＣカードの認証切替プログラムを格納した記憶媒体に係り、特に、ＩＣカードの本人確認を行う場合における認証方法を切り替えるためのＩＣカード及びＩＣカードの認証切替方法及びシステム及びＩＣカードの認証切替プログラムを格納した記憶媒体に関する。
【０００２】
【従来の技術】図１０は、従来のＩＣカードの構成を示す。従来、ＩＣカード１０を利用する場合には、当該ＩＣカード１０を使用する毎に当該ＩＣカード１０の所有者がパスワードを入力することで、本人性の確認を行っている。これによりＩＣカード１０は、ＲＡＭ１１にパスワードが入力されて本人確認された後、使用可能状態となる。使用を終了する場合には、ＩＣカード１０をスロットから引き抜く（全て使用が終了すればＩＣカードは返却口から出てくる）ことで、電源供給が絶たれ、本人確認情報の保持されているＲＡＭは本人確認以前の状態（未認証状態）に戻る。
【０００３】
【発明が解決しようとする課題】しかしながら、上記従来の方法に示すように、本人確認をカード使用の都度行うことは、安全性の観点からは優れているが、利用する毎にパスワードを入力するため、利便性の観点からは本人確認をいちいち行うので面倒であるという問題がある。
【０００４】本発明は、上記の点に鑑みなされたもので、カードの所有者本人が本人確認を済ませた状態でＩＣカードを保持しておく状態と、従来と同様に、パスワード入力がないと使用不可能状態とする２通りの状態を選択することが可能なＩＣカード及びＩＣカードの認証切替方法及びシステム及びＩＣカードの認証切替プログラムを格納した記憶媒体を提供することを目的とする。
【０００５】
【課題を解決するための手段】本発明は、パスワードを入力し、認証することにより使用可能状態となるＩＣカードであって、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、揮発性メモリの内容が複写され、カード引抜き時においても使用可能状態を保持する不揮発性メモリとを有する。
【０００６】図１は、本発明の第１の原理を説明するための図である。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替方法において、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い（ステップ１）、利用者が正当であると認証された場合に、ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込む共に（ステップ２）、不揮発性メモリにも「認証済」を書き込む（ステップ３）。
【０００７】また、本発明は、任意のタイミングで、使用可能状態が書き込まれている不揮発性メモリの内容を、ＩＣカードを使用不可能状態とする「未認証」に書き替える。図２は、本発明の第２の原理を説明するための図である。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替方法において、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い（ステップ１０）、利用者が正当であると認証された場合に、ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込み（ステップ１１）、ＩＣカードの使用時に、不揮発性メモリにも「認証済」を書き込み（ステップ１２）、ＩＣカードの使用後、不揮発性メモリに「未認証」を書き込む（ステップ１３）。
【０００８】図３は、本発明の第１の原理構成図である。本発明は、パスワードが入力され、認証されると使

用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替システムであって、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段２１と、認証手段により利用者が正当であると認証された場合に、ＩＣカードを使用可能状態とする「認証済」をＩＣカードの揮発性メモリに書込み、更に、不揮発性メモリにも「認証済」を書き込む認証情報書込手段２２とを有する。

【０００９】また、本発明のＩＣカード認証切替システムは、任意のタイミングで、使用可能状態が書き込まれている不揮発性メモリの内容を、ＩＣカードを使用不可能状態とする「未認証」に書き替える認証情報書替手段を更に有する。図４は、本発明の第２の原理構成図である。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替システムであって、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段２１と、認証手段により、利用者が正当であると認証された場合に、ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込む揮発性メモリ書込手段２３とを有するバランスリーダ２０と、ＩＣカードの使用時に、不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込手段３３と、ＩＣカードの使用後、不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込手段３４とを有する端末３０とを有する。

【００１０】本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替プログラムを格納した記憶媒体であって、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、認証プロセスにより利用者が正当であると認証された場合に、ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込み、更に、不揮発性メモリにも「認証済」を書き込む認証情報書込プロセスとを有する。

【００１１】また、本発明のＩＣカード認証切替プログラムを格納した記憶媒体は、任意のタイミングで、使用可能状態が書き込まれている不揮発性メモリの内容を、ＩＣカードを使用不可能状態とする「未認証」に書き替える認証情報書替プロセスを更に有する。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替プログラムを格納した記憶媒体であって、ＩＣカードを読み込むバランスリーダに搭載され、ＩＣカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、認証プロセスにより、利用者が正当であると認証された場合に、ＩＣカードを使用可能状態とする「認証済」を揮発性メモリに書込む揮発性メモリ書込プロセスとを有する。

【００１２】本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するＩＣカードを、使用可能状態または、使用不能状態とするＩＣカード認証切替プログラムを格納した記憶媒体であって、ＩＣカードの使用時の端末に搭載され、ＩＣカードの使用時に、該ＩＣカードの揮発性メモリに「認証済」が書き込まれている場合に、不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込プロセスと、ＩＣカードの使用後、不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込プロセスとを有する。

【００１３】上記のように、本発明は、不揮発性メモリと揮発性メモリを使い分けることにより、カードメモリの役割分担をすることで、カードの所有者が、本人確認を済ませた状態でカードを保持しておく場合と、従来のようにパスワード入力がないと使用可能状態にならない状態とを適宜選択できる構造を有する。即ち、ＩＣカード内に揮発性メモリであるＲＡＭと不揮発性メモリであるＥＥＰＲＯＭの領域を設け、最初にパスワードにより本人確認してカード使用可能状態となったものを、ＥＥＰＲＯＭにそのまま保持し、次回からパスワードによる本人確認をしなくてもカードが使用できるようにした。ＥＥＰＲＯＭは、従来本人確認の状態を保持していたＲＡＭと異なり、電源供給が絶たれても、メモリ内容は保持されるので、ＥＥＰＲＯＭに本人確認情報を保持させることで、カード所有者が、この本人確認情報を解除しない限り、本人確認することなくカード使用可能状態となる。但し、任意の時点でカード所有者の指示により、認証状態を解除することができる。

【００１４】また、本発明では、上記において、任意に本人認証を解除できるが、解除しない場合は紛失した際に他人に使用される可能性がある。金額の限界を高く設定しているポストペイドのような場合には、何等かの形でガードをかける必要がある。つまり、ＥＥＰＲＯＭに保持されている本人認証情報を“未認証”にする必要がある。本発明では、ＥＥＰＲＯＭの認証済みの情報を自動的に未認証しているため、紛失してもパスワードの入力がない限り使われることはない。つまり、従来のカードは、パスワード入力を使用直前に端末を用いて入力し

なければならないが、本発明では、ＥＥＰＲＯＭにバランスリーダを用いて自分の家等のプライベートな場所で入力し、ＥＥＰＲＯＭ上に認証済みの情報を保持しておき、店舗で買物等をしてカードを使用し、店舗の端末からカードを取り出す時にはＲＡＭ上にも“未認証”、ＥＥＰＲＯＭ上でも“未認証”の状態となるようにすることで、パスワードを人前で入力することがない上に、使用後は、パスワードの入力なしには使用不能となるため、安全性を増すことができる。

【００１５】

【発明の実施の形態】最初に本発明の第１の実施の形態について説明する。本実施形態では、最初にパスワードにより本人確認を行い、カード使用可能状態となったものを、ＥＥＰＲＯＭにそのまま“使用可能状態”として保持し、次回から本人確認を行わなくとも当該ＩＣカードを利用できる形態であり、プリペイドカード等に適用される場合について説明する。

【００１６】図５は、本発明のＩＣカードの構成を示す。同図に示すＲＡＭ１１には、当該ＩＣカードの使用状態が書き込まれ、バランスリーダから引き抜かれた時点で当該ＲＡＭ１１の内容は消去される。ＥＥＰＲＯＭ１２は、ＩＣカードの使用状態が書き込まれるとバランスリーダからＩＣカードが引き抜かれた場合でも当該書き込まれた情報はそのまま保持される。

【００１７】図６は、本発明の第１の実施形態におけるバランスリーダの構成を示す。同図に示すバランスリーダ２０は、ＩＣカードに対してパスワードを要求し、入力されたパスワードの認証を行う認証部２１と、ＩＣカードの状態を認証状態、未認証状態に切り替える切替制御部２２から構成される。認証部２１は、利用者にパスワードの入力要求を発行し、パスワードが入力されると当該ＩＣカードの状態を未認証状態から認証状態にするために、ＩＣカード１０のＲＡＭ１１を認証済とする。これにより、ＩＣカード１０では、ＲＡＭ１１に書き込まれた“認証済”をＥＥＰＲＯＭ１２に対してコピーし、当該ＥＥＰＲＯＭ１２を認証状態として保持する。

【００１８】切替制御部２２は、上記の認証部２１において“認証済”となっているＥＥＰＲＯＭの状態を未認証にするためのステータスをＩＣカード１０に発行し、ＥＥＰＲＯＭ２２を“未認証”の状態とする。これにより、ＩＣカード１０をスロットから引き抜いた場合でも、ＩＣカード１０には“使用可能状態”が保持されるため、使用時にパスワードを入力する必要がない。

【００１９】次に、本発明の第２の実施の形態を説明する。本実施形態は、ＩＣカードの紛失や盗難に備えて、カード使用後に本人認証情報を“未認証”状態とする形態であり、ＩＣカードが電子現金として利用されるような場合について説明する。図７は、本発明の第２の実施形態における店舗端末の構成を示す。

【００２０】同図に示す店舗端末３０は、ＩＣカード１０が“使用可能状態”（ＩＣカード１０内のＥＥＰＲＯＭ１２の状態が“使用可能状態”）であり、電子現金として使用される場合に、購入した価格をＩＣカード１０の残高から差し引いて、その結果を新残高としてＩＣカード１０の内容を更新する支払制御部３１と、ＩＣカード１０のＥＥＰＲＯＭ１２の状態を“使用可能状態”から“使用不可能状態”に切り替えるステータスをＩＣカード１０に発行する切替制御部３２から構成される。

【００２１】

【実施例】以下、本発明の実施例を図面と共に説明する。

［第１の実施例］まず、第１の実施例として、ＩＣカードとして使用限度額が予め決められているプリペイド型カードを例として説明する。この場合、ＩＣカードの所有者が本人確認を済ませた状態で当該カードを保持するものとする。

【００２２】図８は、本発明の第１の実施例のプリペイドカードの使用例を示すシーケンスチャートである。

ステップ１０１）　まず、バランスリーダ２０がパスワードを取得すると、当該バランスリーダ２０のスロットに挿入されたＩＣカード（プリペイドカード）に記憶されているパスワードと入力されているパスワードとの照合を行い、照合において、一致する場合には、「VERYFY」コマンドを実行して、ＩＣカード１０のＲＡＭ１１に認証情報として“認証済”を書き込む。

【００２３】ステップ１０２）　次に、バランスリーダ２０は、「STORE STATUS」コマンドを実行して、挿入されている当該ＩＣカード１０のＥＥＰＲＯＭ１２に、ＲＡＭ１１の内容（「認証済」）をコピーする。

ステップ１０３）　当該ＩＣカード１０をバランスリーダ２０のスロットから引抜くと、電源ストップによりＲＡＭ１１の内容が自動的に「未認証」となる。

【００２４】ステップ１０４）　当該ＩＣカード１０を所有者が使用する場合には、店舗端末３０に当該ＩＣカード１０を挿入すると、端末３０は、パスワードの入力要求を発行することなく、上位モジュールから「MOVE STATUS」を実行して当該ＩＣカードのＥＥＰＲＯＭ１２の内容をＲＡＭ１１にコピーすることで、当該ＩＣカード１０が使用可能となる。

【００２５】ステップ１０５）　端末３０は、利用者の商品の購入等に対する金額を当該ＩＣカード１０に記憶されている額面から差し引く。

ステップ１０６）　決済が終了した利用者は、端末３０からＩＣカード１０を引き抜くと、電源ストップにより自動的にＲＡＭ１１の内容が「未認証」となる。

【００２６】ステップ１０７）　利用者が自宅等のプライベートな場所に設置してあるバランスリーダ２０に当該ＩＣカード１０を挿入すると、当該バランスリーダ２０は、「CLEAR STATUS」コマンドを発行して当該ＩＣカード１０のＥＥＰＲＯＭ１２の内容を「未認証」に書き

替える。このように、ＩＣカード１０のＥＥＰＲＯＭ１２に「認証済」を書き込んでおくことにより、使用対象の端末においてパスワードの入力を行うことなく、当該端末において、当該カード１０のＥＥＰＲＯＭ１２の内容をＲＡＭ１１にコピーすることにより使用可能となる。また、カード使用者の指示により任意の時点でバランスリーダ２０により認証状態の解除（未認証状態）にすることが可能であるため、所有者が使用しない場合には、バランスリーダ２０に当該ＩＣカード１０を挿入する処理を行うだけで、他人の悪意による使用が不可能となる。

【００２７】［第２の実施例］次に、第２の実施例は、上記の第１の実施例におけるプリペイドカードの場合には、任意に本人認証を解除できるが、解除していない状態において紛失した際に、他人に使用される可能性が残る。特に金額の限界を高く設定しているポストペイドのような場合には、更なるガードが必要となる。

【００２８】本実施例では、ＩＣカードとしてポストペイド（電子現金）の場合を例として説明する。図９は、本発明の第２の実施例のポストペイドの使用例を示すシーケンスチャートである。

ステップ２０１）　バランスリーダ２０のスロットにＩＣカード１０を挿入すると、当該バランスリーダ２０はパスワードの入力を要求し、パスワードが入力されると、当該ＩＣカード１０に記憶されているパスワードと入力されているパスワードとの照合を行う。

【００２９】ステップ２０２）　照合において、一致する場合には「VERYFY」コマンドを実行してＩＣカード１０のＲＡＭ１１に認証情報として“認証済”を書き込む。

ステップ２０２）　次に、「STORE STATUS」コマンドを実行して、バランスリーダ２０は、挿入されている当該ＩＣカード１０のＥＥＰＲＯＭ１２に、ＲＡＭ１１の内容（「認証済」）をコピーする。

【００３０】ステップ２０３）　当該ＩＣカード１０をバランスリーダ２０のスロットから引抜くと、電源ストップによりＲＡＭ１１の内容が自動的に「未認証」となる。

ステップ２０４）　利用者が当該ＩＣカード（ポストペイド）を使用する店舗端末３０のスロットに挿入すると、当該端末３０は、上位モジュールより「MOVESTATUS」コマンドを実行することにより、ＥＥＰＲＯＭ１２の内容（「認証済」）をＲＡＭ１１にコピーする。これにより、当該ＩＣカードが使用可能状態となる。

【００３１】ステップ２０５）　端末３０は、利用者の商品の購入等による決済を行い、当該ＩＣカード（ホストペイド）の残金から決済金額を差し引いて、残金を更新する。

ステップ２０６）　決済が済むと、端末３０は、「CLEAR STATUS」コマンドを実行して、ＥＥＰＲＯＭ１２の内容を「未認証」とする。

【００３２】ステップ２０７）　当該ＩＣカード１０を端末３０のスロットから利用者が引き抜くと、電源ストップによりＲＡＭ１１の内容が自動的に「未認証」となる。このように、店舗端末３０においてポストペイドとしてＩＣカード１０を利用する場合にも、人前でパスワードの入力を行うことなく、当該カードが利用できると共に、利用が終了すると自動的に「未認証」状態となるので、仮に他者が拾って使用しようとしても、パスワードを入力しない限り使用することが不可能となる。

【００３３】また、上記の第１及び第２の実施例では、プリペイドカード、ポストペイドを例としているが、この例に限定されることなく、認証、未認証のモードが必要となるＩＣカード一般に適用可能である。また、図６、図７に示すバランスリーダや店舗端末の各構成要素をプログラムとして構築し、当該装置内のメモリや、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明のようにＩＣカードの認証、未認証により使用を制限する必要があるシステムに汎用的に利用することが可能である。

【００３４】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００３５】

【発明の効果】上述のように、本発明によれば、最初にパスワードにより本人確認を行いカード使用可能状態（「認証済」）となったものを、ＩＣカード内の不揮発性メモリに保持しておくことで、カードリーダから引き抜くことにより電源の供給が絶たれ、揮発性メモリに格納されている本人確認情報が「未認証」であっても、使用時に改めてパスワードを入力することがないため、人前で本来秘密としておくべきパスワードの入力を行う必要がない。

【００３６】さらに、使用後に、利用者の意思により再度不揮発性メモリに書き込まれている「認証済」の状態を「未認証」に書き替えることも可能であり、利用者の意思により適宜いずれかの状態を選択することが可能である。また、本発明によれば、プライベートな場所でパスワードを入力し、不揮発性メモリに「認証済」を保持しておき、当該カードの使用後、当該不揮発性メモリの状態を「未認証」と書き替えることにより、店舗端末からカードを取り出す時点では、揮発性メモリ及び不揮発性メモリの双方が「未認証」状態となるため、と該カードの悪用が回避できる。

【図面の簡単な説明】

【図１】本発明の第１の原理を説明するための図である。

【図２】本発明の第２の原理を説明するための図である。

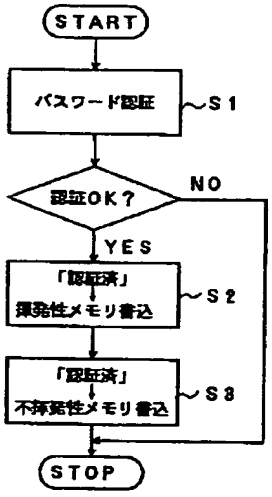
【図３】本発明の第１の原理構成図である。

【図４】本発明の第２の原理構成図である。
【図５】本発明のＩＣカードの構成図である。
【図６】本発明の第１の実施形態におけるバランスリーダの構成図である。
【図７】本発明の第２の実施形態における店舗端末の構成図である。
【図８】本発明の第１の実施例のプリペイドカードの使用例を示すシーケンスチャートである。
【図９】本発明の第２の実施例のポストペイドの使用例を示すシーケンスチャートである。
【図１０】従来のＩＣカードの構成図である。
【符号の説明】

１０　ＩＣカード
１１　ＲＡＭ
１２　ＥＥＰＲＯＭ
２０　バランスリーダ，ＩＣカード認証切替システム
２１　認証部、認証手段
２２　切替制御部、認証情報書込手段
２３　揮発性メモリ書込手段
３０　店舗端末
３１　支払制御部
３２　切替制御部
３３　使用時不揮発性メモリ書込手段
３４　使用後不揮発性メモリ書込手段

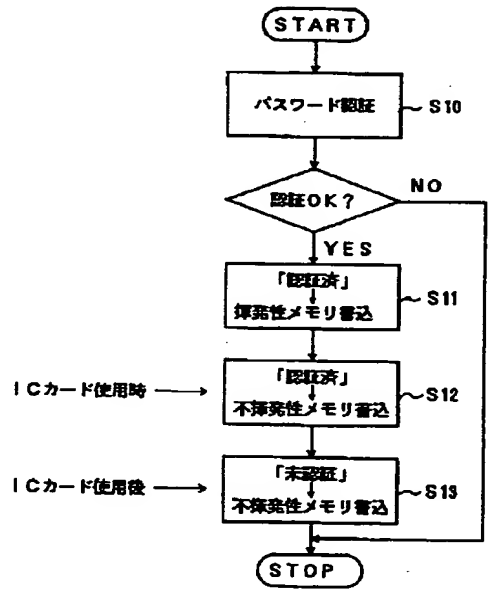
【図１】

本発明の第１の原理を説明するための図



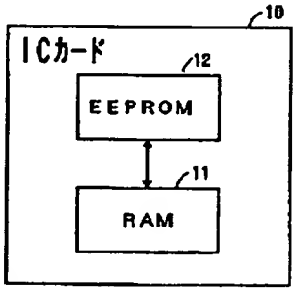
【図２】

本発明の第２の原理を説明するための図



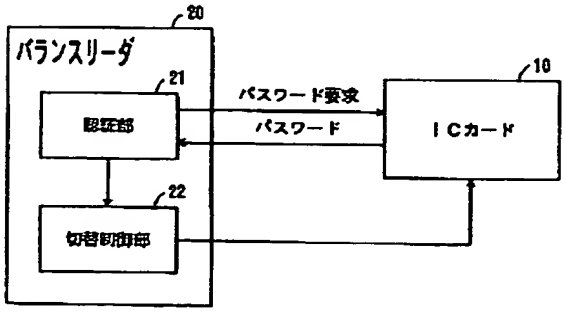
【図５】

本発明のＩＣカードの構成図



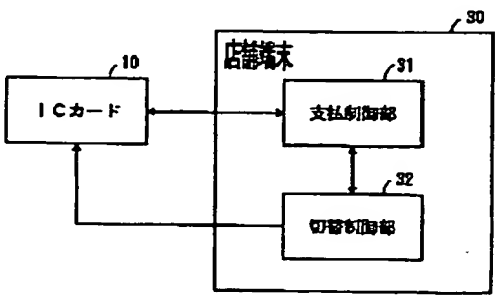
【図６】

本発明の第１の実施形態におけるバランスリーダの構成図



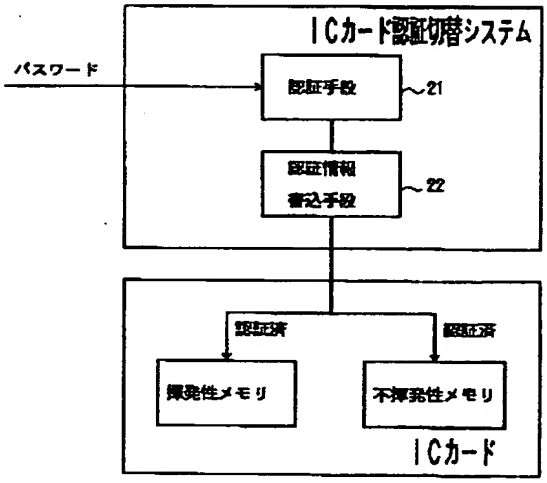
【図７】

本発明の第２の実施形態における店舗端末の構成図



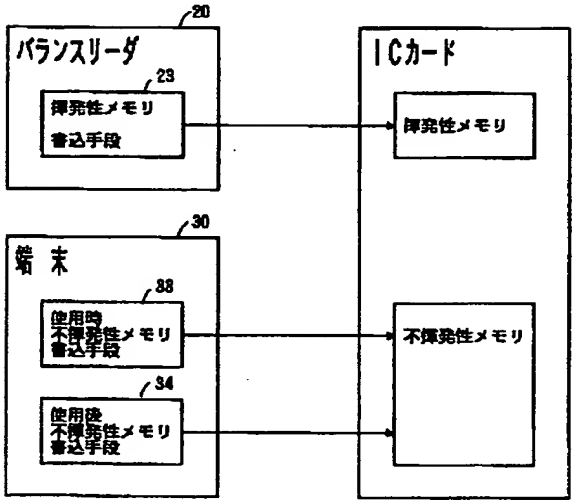
【図３】

本発明の第１の原理構成図



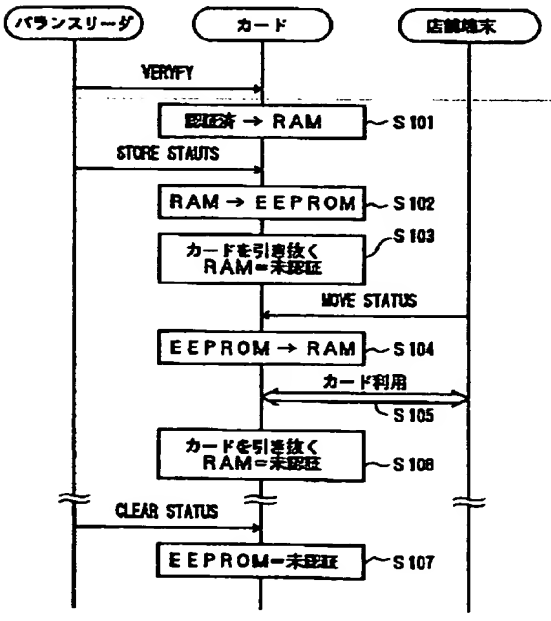
【図４】

本発明の第２の原理構成図



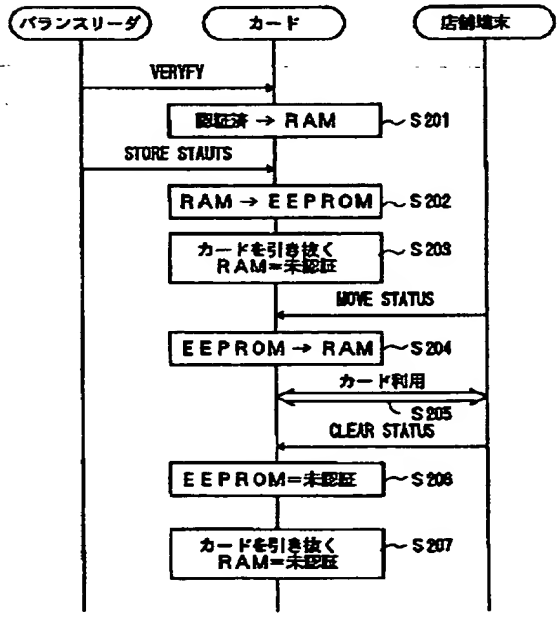
【図８】

本発明の第１の実施例のプリペイドカードの
使用例を示すシーケンスチャート



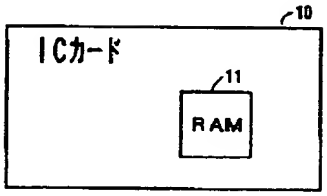
【図９】

本発明の第２の実施例のポストペイドの
使用例を示すシーケンスチャート



【図１０】

従来のＩＣカードの構成図



フロントページの続き

(72)発明者　鈴木　健一
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内